Marella, Venkata; Roshan Kokabha, Maryam; Merikivi, Jani; Tuunainen, Virpi

Rebuilding Trust in Cryptocurrency Exchanges after Cyber-attacks

Published in:
Proceedings of the 54th Hawaii International Conference on System Sciences

Published: 05/01/2021

Document Version
Publisher's PDF, also known as Version of record

Rebuilding Trust in Cryptocurrency Exchanges after Cyber-attacks

Venkata Marella
Aalto University
venkata.marella@aalto.fi

Maryam Roshan
University of Gothenburg
maryam.roshan@ait.gu.se

Jani Merikivi
Grenoble Ecole de Management
jani.merikivi@grenoble-em.com

Virpi Kristiina Tuunainen
Aalto University
virpi.tuunainen@aalto.fi

Abstract

Cryptocurrency exchanges are subjected to cyber-attacks and cryptocurrencies worth millions of US dollars are lost every year. The value of cryptocurrencies is volatile and the cyber-attacks on the exchanges make them even more volatile. Whenever these cyber-attacks happen, the customers might lose their trust not only on a given exchange but also in cryptocurrencies in general. Hence, the exchanges need to rebuild trust among their current and potential customers after a cyber-attack. In this paper, we present findings from a study on cyber-attacks on seven different exchanges, focusing on how they responded after the cyber-attacks to rebuild customers' trust. Analyzing the responses of current and potential customers to the trust rebuilding techniques used by the exchanges, we also assessed the efficiency of these techniques.

1. Introduction

Since the advent of the first cryptocurrency Bitcoin in 2009, cryptocurrencies – defined as digital cash that uses cryptographic algorithms to ensure the safety and the security of the transactions [28][14] – have gained mainstream popularity across the world. Today, there are over 5,000 different cryptocurrencies (e.g. Bitcoin, Ripple, Litecoin, and Tether) with a total market capitalization of around $700 billion [50].

The popularity of cryptocurrencies has also spurred cryptocurrency exchanges, that is, online services through which individuals can buy and sell cryptocurrencies using fiat cash or digital currencies [18]. Today (in 2020), a few hundred exchanges are attending to around 15 million active investors [23]. Apart from exchanging cryptocurrencies, they also provide their customers with cryptocurrency wallets, which are the media used for storing, retrieving, and spending cryptocurrencies.

Given that the exchanges administer millions of wallets worth billions of dollars, they have become attractive targets for sophisticated hackers. Indeed, many exchanges, including those with an established reputation, have lost cryptocurrencies worth several millions of dollars due to cyber-attacks [38]. Therefore, these cyber-attacks pose a major threat to cryptocurrency exchanges, and compromising even a few cryptocurrency wallets will damage their customers' trust in them [6]. When cyber-attacks occur despite preventive efforts, cryptocurrency exchanges need to undertake actions to rebuild the customers' trust to make them continue using their services.

Management literature on trust recovery offers various guidelines (see e.g. [19]), yet none of them is designed particularly for online organizations like cryptocurrency exchanges that have no physical presence and operate fully digitally. However, the exchanges need to understand the necessary steps and requirements to rebuild trust among the customers after cyber-attacks. With this in mind, we state our research question as follows:

How can cryptocurrency exchanges rebuild trust among their current and potential customers after a cyber-attack?

To answer this research question, we draw on the trust repair model proposed by Lewicki and Tomlinson [19]. The trust repair model identifies three key trust regainers: social accounting (i.e., explanations and apologies), compensation (i.e., reparations and penance), and structural solutions. These regainers reflect the steps the trustee has to take to rebuild trust. Since the trust relationships are generally arm's length and transaction-focused, and the trustors' rely heavily on their cognitive assessment [10][30], we believe the model is applicable also in the context of cryptocurrency exchanges.

A study on rebuilding trust is of great relevance to information systems (IS) researchers at least for two reasons. First, while losing trust is arguably harmful to any organization ([12]; [16]; [29]; [32]), it does not always lead to bankruptcy if broken trust can be regained (e.g., [1]; [21]). Yet, research on macro-level trust recovery appears scarce in the IS discipline [1] and virtually non-existent in the cryptocurrency domain. Hence, advancing theorizing about trust recovery by identifying the actions, which help rebuild trust among the existing and potential customers is particularly

URI: https://hdl.handle.net/10125/71304
978-0-9981331-4-0

valuable. Second, due to digital transformation, and especially the consequences of the recent COVID-19 pandemic, we are likely to witness more and more organizations that operate mainly or solely online. Given that these organizations lack physical touchpoints, their trust recovery attempts (e.g., compensation and guarantee policies, trusted party certificates, etc.) call for specific guidelines. While the guidelines our paper offers are intended for cryptocurrency exchanges for rebuilding trust, we believe they are also useful for other online businesses in improving their trust recovery processes.

2. Theoretical Background

2.1. Defining Trust

Trust is defined as the willingness of one party to be vulnerable to the actions of another party with the expectation that the other party will perform the promised action without being monitored or controlled [34]. The party (or the person) who trusts is called a trustor and the party (or the person) who is trusted is called a trustee [26]. Trust has been studied extensively in many disciplines (e.g., biology, economics, philosophy, sociology, psychology, information systems). What academics in different disciplines agree on, is the social grounding of trust (see e.g., [7]; [8]): "*We as humans would not even be able to face the complexities of the world without resorting to trust, because it is with trust that we are able to reason sensibly about the possibilities of everyday life*." ([24], p. 3; [22]). Vu (2010)[43] goes as far as to say that societies would cease to exist without trust.

Trust is described as something that emerges and develops when individuals no longer "*need or want any further evidence or rational reasons for their confidence in the objects of the trust*." [44] (p. 970). Trust is developed by gaining knowledge that helps in the reduction of uncertainties concerning others. Barber [2] (p. 5) writes that *"if one were omniscient, actions could be undertaken with complete certainty, leaving no need, or even possibility, for trust to develop."* Through the development of trust, we try to reduce our vulnerability to others and the uncertainties that entail it [34][25]. Trust will thus give us peace and ease of mind when we are about to put something on the line, such as our time, our financial resources, and, at times, even our reputation [24]. As Uslaner [42] points out, trust is "*a belief about another person's trustworthiness concerning a particular matter at hand that emerges under conditions of unknown outcomes*."

Trust is then tested in reality and sometimes it is violated. While people decide by themselves what and who to trust, Herzberg [13] contends that people tend to blame not themselves but the trustee for any violations. These violations erode trust and the extent to which trustors are not willing to continue cooperating with the trustee. But trust is not necessarily lost, as long as the trustee seeks to take actions that repair it.

2.2. Rebuilding Trust

Trust violations occur when an outcome does not conform to the trustor's expectations of the trustee's behavior [41]. These violations can happen in two ways. First, a trustor can expect trusting behavior and encounter distrust. Second, a trustor can expect distrusting behavior and encounter trust. If the trust violation is significant or if it occurs more regularly, the trustor is going to change his or her perception of trust and alter the relationship with the trustee [20]. Hence, the repair of damaged trust is of the highest practical significance. Trust repair can be regarded as a process of changing the trustor's negative expectations that were accumulated due to a trust violation, to a point where the trustor is once again willing to put his or her confidence in the trustee and become again vulnerable to his or her actions [11]. A general response to trust violations includes social accounting (including explanations and apology), compensation (including reparations and penance), and structural solutions (including regulation and hostage posting) [19].

Many trust repair studies have focused on verbal accounting as a way to repair trust. A study on the apology of trust violation examines two kinds of apologies where in the first approach, the trustee makes an internal attribution of the violation and takes full responsibility for it; In the second approach, the trustee makes an external attribution for the violation and blames someone else for the violation [29]. The research results suggest that internal attribution is more effective when the violation is due to low competence and external attribution is more effective when the violation is due to low integrity [29].

Polin et al. [31] identified six potential components on an effective apology: expression of regret for the violation, explanation of why the violation occurred, acknowledgment of responsibility for causing the violation, declaration of repentance (intent not to commit the violation in the future), an offer of repair (for the damage created by the violation), and request for forgiveness. *Expression of regret* refers to the trustee's expression of regret for the offense. *Explanation of violation* is a statement where the trustee explains how the violation happened to the trustee. *Acknowledgment of responsibility* is a statement where the trustee accepts his part of the mistake. *Declaration of repentance* is a statement where the trustee expresses his sadness for violation and promises not to repeat it. An *offer of repair*

refers to a statement extending a way to work toward trust rebuilding on the part of the trustee. *Request for forgiveness* is a statement asking for the trustor to pardon the trustee's actions. The study concludes that an apology is more effective if it has all of these components. Research on social accounting has concluded that reticence (silence) is a suboptimal response to trust violation [44]. Reticence appears to show an expression of repentance by showing that the trustee is upset about the violation and is willing to change things to prevent further violations [19]. Nevertheless, a recent study concluded that denial of a trust violation is more effective than an apology when the trust violation is due to the low integrity of the trustee [19].

Actions of a trustee play a stronger role in the trust repair process than his or her words [33]. An offering of financial compensation for violations can restore trust. A substantial penance shows a sign of repentance and is considered an effective way to rebuild trust [19]. When the trustee overcompensates the trustor, then it is more likely to repair trust with the trustor [39].

The last category of trust repair techniques is related to the structural change of the situation to minimize trust violations in the future. Nakayachi and Watabe [27] found that hostage posting helps trust repair whereby the trustee allows the trustor to monitor his or her actions and pay penalties for any violations. Similarly, regulation is a tactic that focuses on altering the situation to make the trustee more accountable for his or her actions [9].

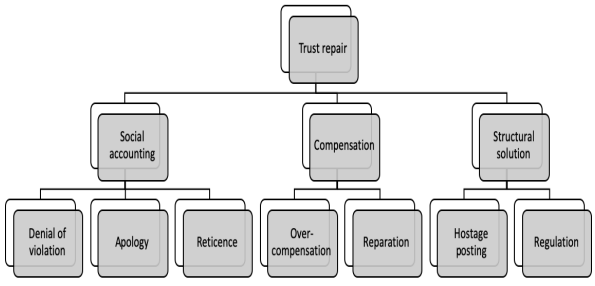

Figure 1. Trust Repair Techniques [19]

3. Data Collection

Our empirical data consists of data on cyber-attacks on cryptocurrency exchanges and customer discussions on these attacks on an online forum dedicated to the discussion of bitcoin, blockchain technology, and cryptocurrency.

We collected data from online cryptocurrency resources (like Coindesk, Cointelegraph, etc.) about major cyber-attacks that occurred on cryptocurrency exchanges between 2012 and 2020. We excluded the DDoS (Distributed Denial of Service) attacks, as they disrupt the operations of the exchange, but do not result in loss of crypto-coins from the online wallets. We also excluded the cyber-attacks that were not discussed extensively on the online forum. Eventually, we selected seven major cyber-attacks on different cryptocurrency exchanges (see Table 2. for the list of studied exchanges).

The main focus of our empirical study was on how these exchanges responded to the cyber-attacks. We gathered information on how they informed their customers about a given cyber-attack, and if, how they apologized for the violation. To communicate their apologies for the cyber-attacks to their customers, the exchanges used various platforms, including e-mail, Twitter, website announcements, and press releases. In addition to the apologies, we also gathered information about other trust rebuilding measures that the exchanges took during the following months after the cyber-attack.

We also focused on how both the current and potential customers responded to these cyber-attacks on Bitcointalk.org, the oldest and the most popular online forum created by Satoshi Nakamoto[1]. The forum is used as a platform for discussion on topics related to cryptocurrencies and exchanges. The forum is used as a platform for discussion on topics related to cryptocurrencies and exchanges. We could deduce that some members of the forum are the customers of the exchange and/or cryptocurrency owners from the statements such as "my wallet is compromised", "my coins", and "my bitcoins". The other posts were viewed as made by potential customers of the exchange. We used 'Beautifulsoup' package in Python for web scrapping the posts made by the current and potential customers of the exchange on the apologies made by the exchanges and analyzed a total of over 500 posts.

[1] The name used by the presumed pseudonymous person or persons who originally developed bitcoin,

4. Research Methodology

We followed a cross-case analysis approach in our empirical study. Cross-case analysis facilitates the comparison of commonalities and differences across different cases [15]. We utilized both quantitative and qualitative methods in our study that consisted of three steps.

Firstly, we used deductive qualitative analysis for the analysis of apologies made by the exchanges, by using the six components of an effective apology proposed by Polin et al. (2012) [31]: an expression of regret, an explanation of violation, an acknowledgment of responsibility, a declaration of repentance, an offer of repair, and a request for forgiveness.

Secondly, we used VADER (Valence Aware Dictionary and sEntiment Reasoner) sentiment analysis to identify the positive and negative sentiments of the user responses to the cyber-attacks. Sentiment analysis is a process through which text is analyzed by using natural language processing (NLP) and the sentiments of text are categorized as negative, positive, or neutral [45]. VADER is a lexicon and rule-based sentiment analysis tool that is specifically attuned to sentiments expressed in social media. For each statement in the text, VADER provides the fraction of positive, negative, and neutral sentiments.

Finally, we focused more deeply on the users' responses for each exchange and conducted a qualitative analysis using the Atlas.ti software. We aimed to identify the factors that contribute to positive and negative sentiments. For this purpose, we started with open coding of the users' responses for each exchange. Next, we clustered the open codes into larger categories that formed meaningful themes.

5. Analysis

We first analyzed the apologies made by the exchanges to their customers after the cyber-attack. We used Polin et al's (2012) [31] research on apology and identified which of the six components of an effective apology are present among the exchanges' apologies. Table 1. presents examples of our coding for the apologies published by the exchanges.

Table 1. Apology Components

Component of apology	Illustrative quote
An expression of regret	"*As much as I regret the post*" (BitFloor Exchange)
An explanation for the violation	*"a few of our servers were compromised"* (BitFloor Exchange)
An acknowledgment of responsibility	*"and expect to recover the loss of the cryptocurrency equivalent"* (Bithumb Exchange)
A declaration of repentance	*"being even more transparent about operations would be a step in this direction if we were to continue operating"* (BitFloor Exchange)
An offer of repair	*"Binance will use the #SAFU fund to cover this incident in full, No user funds will be affected"* (Binance Exchange)
A request for forgiveness	No exchange used this component in their apology.

We next analyzed the data about the customers' response to these cyber-attacks. From the data scrapped from Bitcointalk.org forum, we performed a line-wise sentiment analysis on the data using VADER sentiment analysis. After the VADER analysis that gave us an overall picture of the effectiveness of each chosen approach in terms of percentage of positive sentiments (see Table 2 for details), we read all the customers' responses and identified the positive and negative comments by using Atlas.ti. We followed an open coding process and further categorized the codes into larger categories. The following table represents the results of sentimental analysis and categories of positive and negative codes.

Table 2: Analysis of Customers' (Current and Potential) Responses

Name of the Exchange and Effectiveness of the Approach (Percentage of Positive Sentiments)	**Positive Responses**	**Negative Responses**
BitFloor (55%)	Faith in the Exchange Reputation of Exchange Hope in the Exchange	Asking for hostage posting
Binance (54%)	Appreciation of Compensation Reputation of the Exchange Contingence Fund for Compensation	Doubt the integrity of the exchange
Bithumb (35%)	The reputation of the Exchange	Doubt the integrity of the exchange Leaving Cryptocurrencies Leaving Exchange Negative impact on exchange Repeated Cyber-attack Upset with security policy
Bitcash (33%)	Phishing attack avoided	Doubt the integrity of the exchange Upset with security policy
Bitstamp (24%)	Appreciation of Openness Rebuilding Trust through incentives	Lack of Trust in Exchange
Bitcoinca (56%)	Trust due to openness Trust due to integrity Trust due to Compensation Sympathy for the exchange	Upset with security policy
Coincheck (69%)	Appreciation of Compensation	Doubt on Compensation Magnitude of the Attack Upset with exchange response

6. Findings

In this section, we will discuss the findings for each of the exchanges in more detail.

BitFloor Exchange: The exchange is reputed for its convenient and low service fee. On September 4th, 2012, some of the BitFloor servers got compromised and the attacker gained access to the unencrypted backup wallet [5]. The exchange management was very transparent about the cyber-attack and was constantly in touch with its customers after it. The apology consisted of four components: expression of regret, the explanation for the violation, acknowledgment of responsibility, and declaration of repentance. It also offered compensation for the customers whose wallets were compromised in the cyber-attack. Our findings show that BitFloor received 55% positive sentiment from the users of the Bitcointalk forum.

Several current and potential customers showed faith in the exchange and expressed hope that it would emerge again from the crisis, as demonstrated by the following statements:

"BitFloor will make up the lost coins in due time with regular operations."

"Bitfloor is a helluva lot cheaper and more convenient than the clip joints being called exchanges out there."

"I hope you can recover from this and re-emerge as a viable exchange."

However, some customers were highly upset about the security policies of the exchange and turned to hostage posting mechanism of rebuilding trust. They were disconcerted about having an unencrypted wallet and demanded transparency and monitoring of the security policies:

"But first you need to develop and publish a better security model and have the community scrutinize it."

Binance Exchange: Binance Exchange is one of the biggest cryptocurrency exchanges in the world, a very reputed exchange with a high trading volume. On May 7th, 2019, cybercriminals used a wide variety of attack techniques ranging from phishing to viruses and succeeded in stealing about 7000 Bitcoins from several accounts [17]. The apology made by the exchange management has the components of an explanation for the violation, an offer of repair, and a declaration of repentance. Since they had a contingency fund to cover the losses of cyber-attacks, the customers were not overly concerned about the cyber-attacks:

"It is strong fact that, binance is a dominant exchange and new exchange initiatives are really attracting attention."

"As Binance said, Binance will use #SAFU funds to cover this incident in full."

However, some users of the forum could not believe that a reputed exchange with a sophisticated security system was hacked, so they questioned the integrity of the exchange.

"Binance is a giant market with an extraordinary level of security and it is almost impossible for hackers to do that,according to binary information, it lost 7000 BTC but I honestly doubt that"

Our analysis showed that the reputation of the exchange and their promise to reimburse the losses played a key role in rebuilding trust among the users. Regarding the exchange's response to the cyber-attack, the percentage of positive sentiments among the members of the 'Bitcointalk.org' forum was 54%.

Bithumb Exchange: On March 30, 2019, Bithumb exchange posted on its Twitter account that the operations of the exchange had been temporarily suspended due to a cyber-attack [48]. Bithumb is the largest cryptocurrency exchange in South Korea. Its apology included an expression of regret, acknowledgment of responsibility, and an offer of repair. Though Bithumb Exchange was a reputed exchange, it was subjected to repeated cyber-attacks, which created a significant trust deficit on the exchange:

"It has been hacked for second time for a huge number of EOS and XRP. It was hacked last year also when 30$ million worth crypto was stolen."

"*All crypto exchanges should increase their exchange security level. In the future things like this will not happen again. I am sorry for what is happening now for the exchange*".

Secondly, there was a lack of transparency on the part of the exchange's management about how the cyber-attack had occurred and many of the current and potential customers suspected that it was an "inside job" and questioned the integrity of the employees working for the exchange:

"Inside job is really hard to eliminate. Greed for money is man's nature."

"It's like inside job and funds might have been moved by individuals associated with the company, so the problem is insider job, it's hard to eliminate."

Even though the exchange offered compensation to its customers, the percentage of positive sentiments regarding the exchange's response to the cyber-attack was quite low (35%), evidently because of the lack of transparency and recurrence of the cyber-attacks.

BitCash Exchange: On November 11th, 2013 this Czech cryptocurrency exchange was hacked, and 4000 customers' wallets were compromised, resulting in a loss of bitcoins worth several million Czech crowns [4]. The exchange management announced a very weak apology and no compensation was offered. They showed a sense of fear and anxiety in their apology by saying, "*Unfortunately the nightmare became reality*". Their apology only explained how the violation had occurred. They further mentioned that they had filed a criminal complaint against the cyber-attackers. Customers were perturbed about the weak security policies and not at all confident that cyber-attacker(s) could be caught as promised by the exchange:

*"How the f**k can you file a criminal complaint against an unknown attacker"*

The percentage of positive sentiments among the members of the 'Bitcointalk.org' forum was only 33%. This is consistent with our analysis that shows that BitCash had a weak strategy in rebuilding trust among its customers.

BitStamp Exchange: Bitstamp, which is one of the largest cryptocurrency exchanges, lost around 19,000 Bitcoins after a security breach on January 5th, 2015 [46]. BitStamp believed that one of the wallets that stored the digital credentials for customers, was lost. The apology of the exchange only consisted of the explanation of the violation and an offer of repair through compensation and other financial incentives (reduction in fees) to rebuild trust. Some current and potential customers were happy with the offered compensation and other incentives:

"Bitstamp promised to refund coins, and is now back in operation."

"They are tying to get earn back people's trust by providing them with 0% fee trades and they said that no one will loose his money. Okay! Quite good incentive they took there."

However, many customers were troubled by the repeated cyber-attacks on the exchange:

"Many peoples not going to trust them after many big scams and its alert for many any thing can happen in near future."

A month later BitStamp announced that its developers had devised better security measures to prevent the attacks in the future [37]. Yet, the percentage of positive sentiments on the forum was only 23%.

Bitcoinica Exchange: On March 02, 2012, Bitcoinica Exchange lost 43,554 Bitcoins in a cyber-attack [49]. The security breach happened as a server hosted by a third party got compromised. The exchange management was very transparent about the attack and also promised to reimburse the money to its customers. The apology of the exchange had an explanation for violation and an offer of repair. The users on the forum were happy with the transparency of the exchange. Since the attack reportedly happened because of the negligence of another company, there was sympathy towards the exchange.

"Thanks Bitcoinica for keeping cool and maintain your integrity."

"I hope Linode provides you with all of the compensation."

"I can only imagine how pissed you are at linode."

There were, however, some customers who were unhappy about the security policies of the exchange:

"I mean seriously, could not this whole thing been prevented if the wallet was just encrypted?"

The percentage of positive sentiments related to Bitcoinica on the forum was 56%.

Coincheck Exchange: Coincheck cyber-attack of January 26, 2018, was the biggest cyber-attack in the cryptocurrency industry to date [36]. The Japanese exchange lost 532 million US dollars in the cyber-attack. But, the exchange promised to compensate and fulfilled the promise later. The apology of the exchange had an expression of regret and offer of repair components. The exchange merged with another financial services company called Monex Group after the cyber-attack to stay in business [47].

"*This is good news for all those who have lost money in Coincheck hack, however only fair response would be to pay back the total loss and not only 420$ of 530$ million stolen."*

The percentage of positive sentiments for Coincheck was 69%.

7. Discussion and Implications

After carefully analyzing our research findings, we have significant insights from the study, which we will discuss in this section.

Our findings show that an apology *per se* is not sufficient after a cyber-attack to rebuild trust among the customers of a cryptocurrency exchange. The exchanges need to fulfill the promises made in the apology. BitCash exchange did not apply any other trust rebuilding mechanisms in addition to issuing an apology to its customers and consequently cumulated only 33% positive sentiments from the current and potential customers. The observation contradicts the claim of Tomlinson et al. [40], that an apology where the offender accepts the full responsibility of the trust violation is good enough to rebuild trust, but supports Schweitzer et al. [35] who concluded that a mere apology will not likely lead to trust repair.

When a cyber-attack occurs, it creates a trust deficit on the exchange. The extant literature [9][28] talks about regulation and hostage postings as structural solutions to rebuild trust [30]. Another type of structural change that could help in rebuilding trust among customers is a merger with a reputed company. Coincheck exchange was subjected to the biggest cyber-attack in history [36]. Despite the magnitude of the cyber-attack, the exchange was willing and able to fully compensate all of its customers. Later, they merged with Monex Group, a financial services company, which further aided in rebuilding trust among the customers [47].

Our research suggests that compensating the customers plays a major role in rebuilding trust, supporting the claim of Bottom et al. [3] that financial compensation would better restore trust among the customers compared to an apology alone. Our findings show that the exchanges that promised compensation in the apology statement as well as explained the exact way they were going to compensate generated sentiments from the customers. These exchanges and their positive sentiments were Binance (54%), Coincheck (69%), Bitcoinica (56%), and BitFloor (55%). This is in line with what earlier research [3][39] has found that compensation leads to greater trust repair. Despite the major role of compensation in rebuilding trust, our findings indicate that if the frequency of the cyber-

attacks is high, even compensations may not be able to rebuild the customers' trust. Bithumb and BitStamp are the exchanges that compensated their customers after a cyber-attack. Yet, they received 35% and 24% positive sentiments from the responses of the current and potential customers respectively. The existing literature [3][39] suggests that compensation is an efficient technique to rebuild trust. However, the findings of our study imply that compensation might be an inefficient technique if there is a repetition of trust violation. In the same vein, our study shows that changing the security policy after a cyber-attack and make some of the customers monitor the security policy more closely is a way to rebuild trust. Some of the customers of the exchanges with required technical skills can monitor the security policies of the exchange regularly. In the case of Bitfloor and Bithumb, many customers demanded the exchanges to make changes to their security policies. The users of the Bitcointalk.org forum propose what Kramer and Lewicki [33] suggest to change the structure of the situation to minimize the trust violations.

Our research findings also show that overall, the reputation of exchange plays an important role in rebuilding trust. Reputed exchanges are not severely impacted by low-magnitude cyber-attacks, as was the case with the Binance exchange. The exchange has a good reputation for protecting customers' wallets against cyber-attacks and they have a separate fund set aside to compensate the customers when necessary. Accordingly, the exchange received 54% positive sentiments from the forum users. Similarly, Bitfloor received 55% positive sentiments from forum users', in all likelihood aided by the reputation of the exchange.

Our paper contributes to the literature of rebuilding trust in organizations that operate completely online without a physical presence in general and specifically for cryptocurrency exchanges. The existing literature proposes regulation [9] and hostage posting [27] as structural solutions to rebuilding trust. Our study highlights the merger as an additional trust rebuilding technique if the organization is hit by a crisis like a cyber-attack. An organization can rebuild trust among their customers by merging with a reputed organization. Coincheck is the only exchange that used a merger to rebuild trust and it received the highest level of positive sentiments among all exchanges. Hence, the efficiency of the merger as a trust rebuilding technique should be studied further.

Our research provides valuable guidelines for the cryptocurrency exchanges to rebuild trust among their current and potential customers after a cyber-attack. Firstly, it is essential for the exchanges to be transparent about the cyber-attacks, also to avoid accusations of an inside job. Secondly, the exchanges should compensate the customers after cyber-attack to rebuild trust among them and it is important to be transparent about the sources of compensation. The exchanges should inform their customers about the compensation already in the initial apology after a cyber-attack. Thirdly, exchanges should review their security policy whenever a cyber-attack happens. Exchanges should inform the customers about the security policy changes and allow them to review the security policies. Finally, cryptocurrency exchanges operate online with no physical touchpoints for interacting with customers. Hence, it is recommended the exchanges make an effective apology with all the six components mentioned by Polin et al. [31] to create a strong foundation to rebuild trust.

When a cyber-attack occurs, exchanges suspend their operations in order to contain the cyber-attack and to reduce the magnitude of damages. However, from a customer's point of view, their exchange has been hacked and they would want to check their wallets to make sure their accounts are safe but the inability to access their accounts will create frustration. Suspending the operations in the face of a cyber-attack is, however, inevitable for the exchanges. Hence, the exchanges need to mention the (estimated or expected) duration for which they will be inactive and explain that it is a measure to protect their wallets from the attack.

8. Limitations and Future Research

Our research has limitations. Our empirical data is secondary data, in the form of public apology statements of the exchanges after they had been attacked, and customer discussions on the attacks and the responses by the exchanges on 'Bitcointalk.org' public forum. One evident limitation is that we were not able to distinguish the actual current customers from potential customers. While our findings shed light on the techniques and their combinations that are important and efficient in rebuilding trust, more research is called for. One potential avenue for future research is to study exclusively the actual customers using primary data collection techniques, and this way we can extend our understanding of customers' response to trust rebuilding techniques by cryptocurrency exchanges.

9. References

[1] Bansal, G., and F.M. Zahedi, "Trust violation and repair: The information privacy perspective", Decision Support Systems 71, 2015, pp. 62–77.

[2] Bernard Barber, The Logic and Limits of Trust, Rutgers University Press, 1983.

[3] Bottom, W.P., K. Gibson, S.E. Daniels, and J.K. Murnighan, "When talk is not cheap: Substantive penance and expressions of intent in rebuilding cooperation", Organization Science 13(5), 2002, pp.

497–513.
[4] bradbury, D., “Czech bitcoin exchange Bitcash.cz hacked and up to 4,000 user wallets emptied”, Coindesk, 2013. https://www.coindesk.com/czech-bitcoin-exchange-bitcash-cz-hacked-4000-user-wallets-emptied
[5] Buterin, V., “Bitfloor Hacked, $250,000 Missing”, Bitcoin Magazine, 2012. https://bitcoinmagazine.com/articles/bitfloor-hacked-250000-missing-1346821046
[6] Caporale, G.M., W. Kang, G. Maria, W. Kang, F. Spagnolo, and N. Spagnolo, “Cyber-attacks and Cryptocurrencies”, (2003), 2020.
[7] Coleman, C.H., “Vulnerability as a Regulatory Category in Human Subject Research”, The Journal of Law, Medicine & Ethics 37(1), 2009, pp. 12–18.
[8] Deutsch, M., The resolution of conflict: Constructive and destructive processes, Yale University Press, 1973.
[9] Dirks, K.T., P.H. Kim, D.L. Ferrin, and C.D. Cooper, “Understanding the effects of substantive responses on trust following a transgression”, Organizational Behavior and Human Decision Processes 114(2), 2011, pp. 87–103.
[10] Dirks, K.T., R.J. Lewicki, and A. Zaheer, “Reparing Relationships Within and Between Organizations: Building A Conceptual Foundation”, Academy of Management Review 34(1), 2009, pp. 68–84.
[11] Dirks, K.T., R.J. Lewicki, A. Zaheer, and K.T. Dirks, “Introduction to Special Topic Forum : Repairing Relationships within and between Organizations : Building a Conceptual Foundation REPAIRING RELATIONSHIPS WITHIN AND BETWEEN ORGANIZATIONS : BUILDING A CONCEPTUAL FOUNDATION”, Academy of Management Review 34(1), 2018, pp. 68–84.
[12] Gillespie, Nicole; Dietz, G., “TRUST REPAIR AFTER AN ORGANIZATIONLEVEL FAILURE”, 34(1), 2009, pp. 127–145.
[13] Hertzberg, L., “On the attitude of trust”, Inquiry 31(3), 1988, pp. 307–322.
[14] Kazan, E., C.W. Tan, and E.T.K. Lim, “Value creation in cryptocurrency networks: Towards a taxonomy of digital business models for bitcoin companies”, Pacific Asia Conference on Information Systems, PACIS 2015 - Proceedings(January), 2015.
[15] Khan, S., and R. Vanwynsberghe, “Forum Qualitative Sozialforschung/Qualitative Social Research Online Forum: Cultivating the under-mined: Cross-case analysis as knowledge mobilization”, 9(1), 2008, pp. 1–18.
[16] Kim, P.H., D.L. Ferrin, C.D. Cooper, and K.T. Dirks, “Removing the Shadow of Suspicion: The Effects of Apology Versus Denial for Repairing Competence- versus Integrity-Based Trust Violations”, Journal of Applied Psychology 89(1), 2004, pp. 104–118.
[17] Lam, E., “Hackers Steal $40 Million Worth of Bitcoin From Binance Exchange”, 2019. https://www.bloomberg.com/news/articles/2019-05-08/crypto-exchange-giant-binance-reports-a-hack-of-7-000-bitcoin
[18] Leighton, B., “What is a cryptocurrency exchange and how do they work?”, Coininsider, 2019. https://www.coininsider.com/cryptocurrency-exchanges/
[19] Lewicki, R.J.., and E.C. Tomlinson, “Trust, Trust Development, and Trust Repair”, In The Handbook of Conflict Resolution : Theory and Practice. 2014, 104–137.
[20] Lewicki, R.J., and B.B. Bunker, “Developing and Maintaining Trust in Work Relationships”, Trust in Organizations: Frontiers of Theory and Research(January 1996), 2012, pp. 114–139.
[21] Liao, Q., X. (Robert) Luo, A. Gurung, and W. Shi, “A Holistic Understanding of Non-Users’ Adoption of University Campus Wireless Network”, Comput. Hum. Behav. 49(C), 2015, pp. 220–229.
[22] Luhmann, N., “1979 Trust and power. Chichester: Wiley”, 1979.
[23] Makarov, I., and A. Schoar, “Trading and arbitrage in cryptocurrency markets”, Journal of Financial Economics(782), 2019.
[24] Marsh, S.P., “Formalizing Trust as a Computational Concept B2-Formalizing Trust as a Computational Concept”, Stirling, Scotland, UK: University of Stirling(April), 1994.
[25] Moody, G.D., D.F. Galletta, and P.B. Lowry, “When trust and distrust collide online: The engenderment and role of consumer ambivalence in online consumer behavior”, Electronic Commerce Research and Applications 13(4), 2014, pp. 266–282.
[26] Naber, A.M., S.C. Payne, and S.S. Webber, “The relative influence of trustor and trustee individual differences on peer assessments of trust”, Personality and Individual Differences 128(June 2019), 2018, pp. 62–68.
[27] Nakayachi, K., and M. Watabe, “Restoring trustworthiness after adverse events: The signaling effects of voluntary ‘Hostage Posting’ on trust”, Organizational Behavior and Human Decision Processes 97(1), 2005, pp. 1–17.
[28] Oshodin, O., A. Molla, and C.E. Ong, “An information systems perspective on digital currencies: A systematic literature review”, Proceedings of the 27th Australasian Conference on Information Systems, ACIS 2016, 2016.
[29] Peter, H.K., K.T. Dirks, C.C. D., and D. L, “When more blame is better than less: The implications of internal vs. external attributions for the repair of trust after a competence- vs. integrity-based trust violation”, Elsevier 99(1), 2006, pp. 49–65.
[30] Peter T. Coleman (Editor), Morton Deutsch (Editor), E.C.M. (Editor), The Handbook of Conflict Resolution: Theory and Practice, 2014.
[31] Polin;, B., R.B. Lount;, and R.J. Lewicki, “On the importance of a full apology: How to best repair broken trust”, Academy of Management Proceedings 1, 2012.
[32] Roderick M. Kramer; Todd L. Pittinsky, Restoring Trust in Organizations and Leaders: Enduring Challenges and Emerging Answers, Oxford University Press, 2012.
[33] Roderick M. Kramer and Roy J. Lewicki, “Repairing and Enhancing Trust: Approaches to Reducing Organizational Trust Deficits”, Academy of Management Annals 4(1), 2010.
[34] Roger C. Mayer, J.H.D. and F.D.S., “An Ingetrative Model of Organizational Trust”, Academy of

Management 20(3), 1995, pp. 709–734.
[35] Schweitzer, M.E., J.C. Hershey, and E.T. Bradlow, “Promises and lies: Restoring violated trust.”, Organizational Behavior and Human Decision Processes 101(1), 2006, pp. 1–19.
[36] Shane, D., “$530 million cryptocurrency heist may be biggest ever”, 2018, 2018. https://money.cnn.com/2018/01/29/technology/coincheck-cryptocurrency-exchange-hack-japan/index.html
[37] Srivastava, S.N., “Bitcoin exchange Bitstamp suspends service after security breach”, Reuters, 2015. https://www.reuters.com/article/us-bitstamp-cybersecurity/bitcoin-exchange-bitstamp-suspends-service-after-security-breach-idUSKBN0KF0UH20150106
[38] Su, J., “Hackers Stole Over $4 Billion From Crypto Crimes In 2019 So Far, Up From $1.7 Billion In All Of 2018”, 2019. https://www.forbes.com/sites/jeanbaptiste/2019/08/15/hackers-stole-over-4-billion-from-crypto-crimes-in-2019-so-far-up-from-1-7-billion-in-all-of-2018/#3d65886055f5
[39] T.M.Desmeta, P., E. VanDijkb, and D. DeCremerac, “In money we trust? The use of financial compensations to repair trust in the aftermath of distributive harm”, Elsevier 2, 2011, pp. 75–86.
[40] Tomlinson, E.C., and R.J. Lewicki, “Trust and trust building”, 2002.
[41] Tomlinson, E.C., and R.C. Mryer, “The Role Of Causal Attribution Dimensions In Trust Repair”, Academy of Management Review 34(1), 2009, pp. 85–104.
[42] Uslaner, E.M., The moral foundations of trust, Cambridge University Press, 2002.
[43] Vu, L.-H., “High Quality P2P Service Provisioning via Decentralized Trust Management”, Analysis 4711(March), 2010.
[44] Weitzl, W., W. Weitzl, and Berg, Measuring electronic word-of-mouth effectiveness, Springer, 2017.
[45] White, B., “Sentiment Analysis: VADER or TextBlob?”, medium.com, 2020. https://towardsdatascience.com/sentiment-analysis-vader-or-textblob-ff25514ac540
[46] Whittaker, Z., “Bitstamp exchange hacked, $5M worth of bitcoin stolen”, zdnet, 2015. https://www.zdnet.com/article/bitstamp-bitcoin-exchange-suspended-amid-hack-concerns-heres-what-we-know/
[47] Wood, A., “Confirmed: Monex Group To Acquire Coincheck”, Cointelegraph, 2018. https://cointelegraph.com/news/confirmed-monex-group-to-acquire-coincheck
[48] Zhao, W., “Crypto Exchange Bithumb Hacked for $13 Million in Suspected Insider Job”, Coindesk, 2017. https://www.coindesk.com/crypto-exchange-bithumb-hacked-for-13-million-in-suspected-insider-job
[49] “Bitcoinica lost 43,554 BTC from Linode compromise, suspicious TXIDs publicized”, bitcointalk.org, 2012. https://bitcointalk.org/index.php?topic=66979.120
[50] “CoinMarketCap”, 2020. www.CoinMarketCap.com